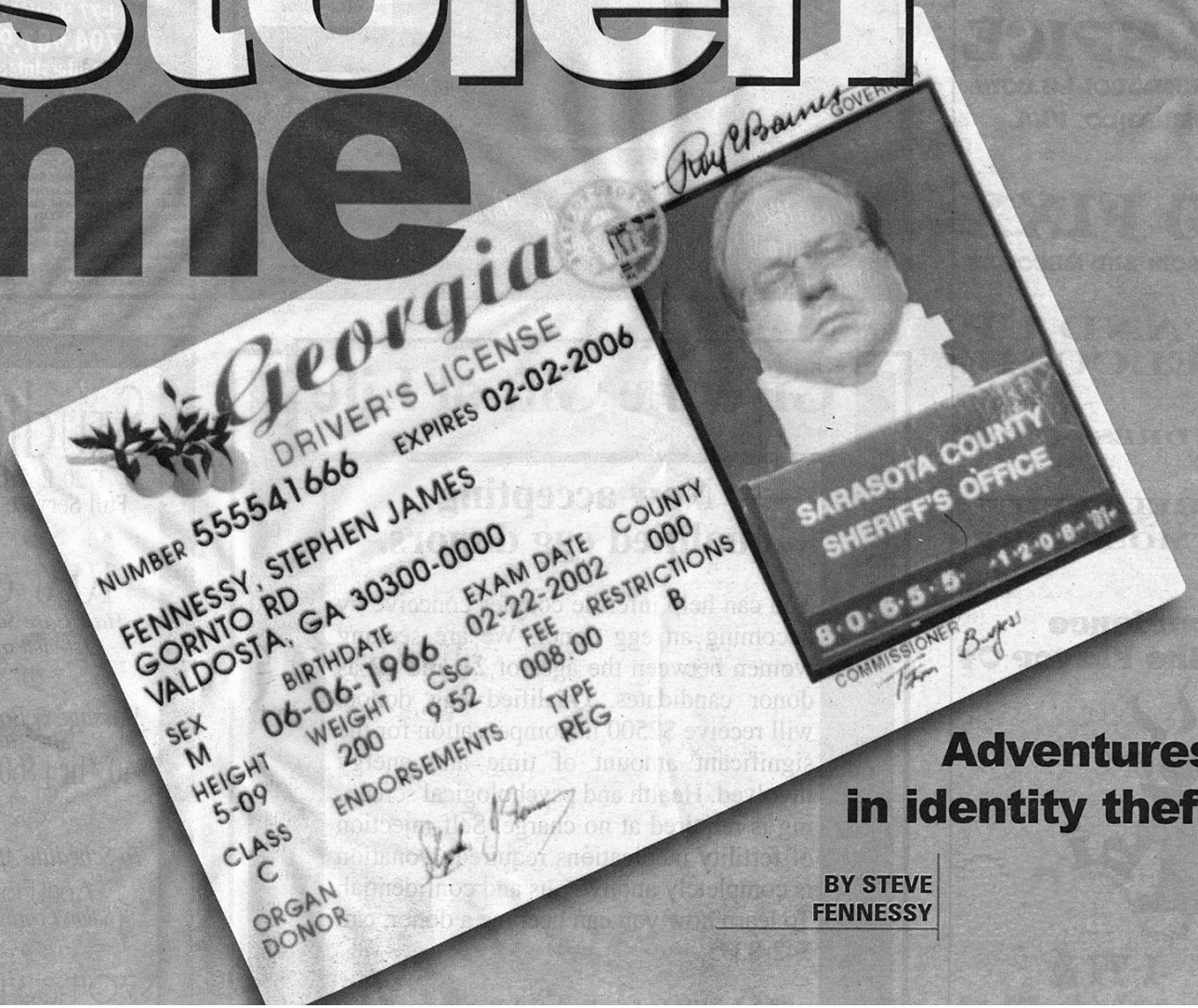
Identity Theft & Fraud in Banking
Protecting Yourself and Your Business

15th Annual Government Financial Management Conference
Bethesda, MD
August 9, 2005

Presenters:
Brian McGinley, Senior Vice President
Director of Loss Management
Wachovia Corporation
(704) 590-4108

The stolen me



Adventures in identity theft

BY STEVE FENNESSY

It happens every day.....

From Talkleft.com 3/9/05

LexisNexis

Lexis-Nexis Database Hacked, Customer Files Accessed

Choice Point is not alone. **LexisNexis**, through its parent company, **Reed Elsevier**, announced today that a **database it acquired from Seisint has been hacked** and up to 32,000 files with personal information have been breached.

FTC: Identity theft strikes 1 in 8 adults

Report says thieves cost $53 billion last year

By Jeordan Legon
CNN
Wednesday, October 29, 2003 Posted: 1:01 PM EST (1801 GMT)

Laptop with Bank R.I. Information Stolen from Fiserv Employee

From: American Banker
Friday, December 19, 2003

Chicago Tribune
ONLINE EDITION
January 20, 2004
19° F

Writers Series Offerings include: Business Grammar Memoir Professional Creative UIC

Hello, VHB54 | MyNews | Log out Story search: Last 7 days Go Older than 7 days

Classified | Ads
Find a job
Find a car
Find real estate
Rent an apartment
Find a mortgage
Shop newspaper ads
White/yellow pages
Personals
Place an ad
Weather | Traffic

Identity theft growing fast, takes time to untangle

You're not alone if bad things happen to your good name

By Lorene Yue
Your Money staff writer
Published January 18, 2004

E-ma
Print

Press Herald ONLINE NEWS

HOME - NEWS - SPORTS - BUSINESS - VIEWPOINTS - OBITUARIES - CLASSIFIEDS - SPECIAL REPORTS - PERSONALS - ARCHIV

Tuesday, January 6, 2004

E-mail this story to a friend

Official warning: Identity theft growing in Maine

By JOSHUA L. WEINSTEIN, Portland Press Herald Writer

DSW Data Theft Much Larger Than Estimated

Tue Apr 19,10:05 PM ET

DSW

COLUMBUS, Ohio - Thieves who accessed a DSW Shoe Warehouse database obtained 1.4 million credit card numbers and the names on those accounts — 10 times more than investigators estimated last month.

CONSUMER REPORTS ● OCTOBER 2003

Dumpster-Diving for Your Identity

Stephen Massey ran a lucrative identity-theft ring that victimized hundreds. You might want to think twice about throwing your old bills away.

By Stephen Mihm

THE NEW YORK TIMES MAGAZINE / DECEMBER 21, 2003

ChoicePoint

Burned By ChoicePoint Breach, Potential ID Theft Victims Face a Lifetime of Vigilance

Feb. 24, 2005

More than 9.9 million Americans were victims of identity theft last year. Many victims are dumbfounded by the dearth of federal and state laws aimed at protecting their credit histories and other information about them.

By Rachel Konrad, AP Technology Writer

Ali Baba was a fortunate man indeed . . . he had but 40 thieves to contend with

C. P. Security Service, Inc.

Financial Fraud Losses

Question:

How Much?

Financial Fraud Losses

Answer: A Lot!

$50+ Billion Annually

Who’s At Risk?

You,

Me

and

Our Businesses!

Welcome to the “Darkside”

Key Tenets of Successful Loss Risk Management & Understanding Risk

- The “Field of Schemes” – Build it and they will come!
  - Recognize that there are people out there trying to steal your business from you.

- Every Product & Process (and modifications there to) has internal and external theft ramifications as well as operating error exposure that must be balanced with control, detection, and audit capabilities.

- We must examine and understand the systems and supporting processes from “end-to-end” to identify potential vulnerabilities. We must understand existing and newly emerging threats to the technology – it is a very dynamic and often hostile environment.

Welcome to the “Darkside”

Key Tenets of Successful Loss Risk Management & Understanding Risk

•What you don’t know can and will hurt you – it not a matter of “if” but rather of “when”!! - “Pay me now or Pay Big Later!”

•In the Risk Arena - Don’t Look To the Past To Determine the Future – Learn from the past – but don’t predict from it.

•Complacency Kills! – Don’t underestimate your adversary or “Mr. Murphy.”

•Reputational Risks - Strong control and loss prevention postures are key to protection of our products and services - even our “Brand.”

•Regulatory Risks – Heavy Emphasis on customer verification, identity theft, customer privacy & authentication

•Litigation Exposures – Some Brave New Worlds out there

Fraud Trends

- **Bank Fraud will continue to increase driven by:**
  - Increased competition – intense focus on bringing new business through the door
  - Reg CC Check Hold Limitations vs. True Check Return Processing Time
  - Expansion of Access Opportunities, New Technology, and Speed - New Products and Product Functionalities
  - Expansion of criminal elements
    - Organized Crime
    - Street Gangs
    - Local, Regional, National & International Fraud Rings
    - Terrorist Financing Opportunity
    - Active Placement and/or Recruitment of insiders with access to customer information
  - Limited risk of immediate detection and apprehension

Fraud Trends

- **Counterfeiting of checks, identification, documentation and access devices is a major exposure area. This has carried over to the electronic environment.**

Level of sophistication has increased significantly and is supported by enhancement and availability of technology and access to supporting information:

- PC document scanning/laser printing
- PC Check Printing Packages with MICR Ink
- Color copiers
- Plastic Embosser / Mag Stripe duplicator

Fraud Trends

- **Access to customer and proprietary information**
  - Internal data compromise
  - External data compromise

Information = Transactional Access

Consumer information and privacy is under siege by individuals who are able to gain access to personal biographic, demographics and financial information via theft of trash, internet, public record sources, compromise of non-public sources via hacking and/or “social engineering” & corruption of individuals with access to the information.

Fraud Trends

- **New Technology – New Opportunities**
  - PC Banking & Expanded Functionality – "Bank in a Box"

    Makes Bank reliant on and vulnerable to – a customer's unsafe computing practices

  - The Internet – "*Reach out and touch someone.*"
  - Electronification – ACH conversation & presentation of checks and return deposits.
    - *Check R&T + Account Number = electronified check, ACH or Draft*
    - *Watch out for Merchant and Merchant employee collusion*
  - eCommerce – a world of new payment mechanisms
  - 3rd Party Aggregators – "Partying With Third Parties" – InfoSec Risk
  - Wireless – PCs, Palms and Cells

- **True Name Identification Takeovers / Impersonations / Identity Theft**

Fraud Containment Challenges

- **Traditional Bank Customer Verification Tools Widely Compromised**
  - Personal ID, Personal Information, Signature Verification, Checks, Plastics, Business Documentation and Reference Letters
- **Globalization of Customer Base**
  - Difficult Verification and Due Diligence for Émigré and Foreign Business
  - Allows for attacks to be launched from anywhere in the world

Fraud Containment Challenges

- **More Access Channels – Many No Longer Under Direct Bank Control**
  - ATM – Proprietary, Networked, Privately Owned
  - POS Expansion
  - Telephone Banking & Bank By Mail
  - PC Banking
  - Internet
  - ACH – now allows direct access to customer accounts by merchants – both bank customer merchants and non-customer merchants via their respective bank (ala ODFI and RDFI)
  - 3rd Party Aggregation & Merchant Processors

- **Remote Identification of Customers – A Continuing Challenge**
  - Bank By Mail
  - Telephone Banking
  - PC / Home Banking
  - Availability of correct bio/demo information
  - Availability and customer acceptance of unique remote identification information and options

Fraud Containment Challenges

- **Counterfeit Checks on the Rise**

  - On-Us Checks – Business, Payroll, Personal
  - Other Deposited Checks – Off-Us, Official Checks, etc.
  - Technology in the hands of the criminals
  - Reg CC – Check Deposit Hold Requirements
  - Impact in electronification environment provides that Routing and Transit Number + Account Number = Electronified Check
  - Unauthorized Signature Drafts

Fraud Containment Challenges

- **Counterfeit Checkcard / ATM Cards**

A major problem that is escalating

- Customer card number and PINs are being compromised by both low tech and high tech schemes

22 YT THE NEW YORK TIMES **NATIONAL** SUNDAY, AUGUST 3, 2003

As A.T.M. System Booms, So Do Thefts From Bank Acc

Stealing at Automated Teller Machines

Criminals use a number of devices to steal from A.T.M. users, usually by capturing their bank account numbers and personal identification numbers.

SKIMMING DEVICES

The authorities say criminals bought this brand of A.T.M. and placed a device inside that captured, or skimmed, bank account numbers and PIN's of thousands of New Yorkers.

FAKE KEYPADS

This keypad was placed over a real A.T.M. keypad, allowing thieves to record PIN's without opening the machine.

VIDEO CAMERAS

Tiny hidden cameras capture the PIN's of unsuspecting A.T.M. users, transmitting those numbers to thieves waiting outside.

FALSE FRONTS

A false front is constructed so that it fits snugly over the outside of a real bank A.T.M. It includes a fake card reader and a touch screen that records PIN's.

Fraud Containment Challenges

- **All ATM, Checkcard and Credit Card MAG Stripe Technology Vulnerable**
  - Primary Sources of Compromise are POS Terminals in Convenience Stores, Grocery Stores, Gas Stations, Restaurants
  - Bogus ATMs and ATM Compromise
  - Phony ATM Fronts & ATM Vestibule Door Access Devices that skim MAG Stripe
  - Use of Camcorder and RF Video Transmission

Fraud Containment Challenges

- **New Frontiers Convergence – Some Volatile Combinations**
  - New Technology
  - New Legal Issues, new laws, no laws, lack of litigation findings
  - Lack of Experience – Lack of Experts
  - A Handful of Electrons – Investigate and Prosecute this!!!
  - Check 21
  - Image – No Originals – Manipulation – Beyond a Reasonable Doubt
- **Outsourcing and Utilization of Temporary Employees**
  - "Who is Minding Our Stores?"
  - Administrative
  - Production Shops, Mail Rooms, Copy Centers
  - PC and LAN Support
  - Security
  - Janitorial
  - Other

Internet Fraud Considerations

Prevalent Internet Schemes:

- Phishing & Pharming
- Web Site Impersonations (Spoofing) – Collection of Account & Authentication Information
- Identity Theft/Customer Impersonation – Establishment of New Account & Remote Authentication Challenges
- Virus Infection – at customer site or bank
- Key Stroke Capture
- Worms
- Denial of Service Attacks
- Session Hijacking
- Breach of Credit Card & Merchant Sites for theft of customer and account information – followed by fraudulent transactions & card counterfeiting
- Packet Sniffing – customer, employment, transmission site or bank
- Use of Remote Access PC Programs – (PC Anywhere – Timbuktu, etc)
- Web Vandalism or redirection links
- Fraudulent Notification or Requests for Information

Protect Your Computer

Your computer can be a goldmine of personal information to a thief.

- Update your virus protection software regularly. Keep your computer up-to-date by installing patches and security repairs you can download from your operating system's Web site.
- Protect your Password and access credentials.
- Don't download files from strangers or click on hyperlinks from people you don't know.
- Use a firewall, especially if you have a high-speed or "always on" connection to the Internet. The firewall allows you to limit uninvited access to your computer.
- Use a secure browser – software that encrypts or scrambles information you send over the Internet – to guard the safety of your online transactions. When you're submitting information, look for the "lock" icon on the status bar and "https" in the URL. It's a symbol that your information is secure during transmission.
- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a "strong" password – that is, a combination of letters (upper and lower case), numbers, and symbols.

Protect Your Computer

- Avoid using an automatic log-in feature that saves your user name and password; and always log off when you're finished. If your laptop gets stolen, the thief will have a hard time accessing sensitive information.
- Delete any personal information stored on your computer before you dispose of it
- Use a "wipe" utility program, which overwrites the entire hard drive and makes the files unrecoverable – when disposing of your PC.
- Read Web site privacy policies. They should answer questions about the access to and accuracy, security, and control of personal information the site collects, as well as how sensitive information will be used, and whether it will be provided to third parties.
- Understand the vulnerabilities of your electronic environment.
  - Remote access is risky
  - Software – like PC Anywhere /Timbuktu. If you use it – set it up right!
  - Wireless?? Very vulnerable. Again – set it up right!

Internet Fraud In the News

May 8, 2003

First Union Hoax on the Loose

eWeek

By Dennis Fisher

A hoax e-mail purporting to come from First Union Bank and attempting to dupe recipients to visit a malicious Web site is making the rounds on the Internet.

The e-mail arrives from the address bankaccount@firstunion.com and informs the recipient that the bank has lost the recipient's online banking username and password. It directs users to a Web site where they are encouraged to enter their usernames and passwords, which are presumably then collected for later use by the scam artist who created the e-mail.

Bank officials say they're trying to determine who is sending the e-mails.

Even if users don't enter their personal information in the form at the site, they could still be at risk. Simply visiting the site triggers an automatic download of the Backdoor-AMQ Trojan horse program to the visitor's machine, according to an advisory published Thursday by the Unified Incident Reporting and Alert Scheme, the U.K. equivalent of the CERT Coordination Center.

Backdoor-AMQ is a well-known application that gives an attacker the ability to remotely control infected machines. Once installed a PC, the program allows an attacker to perform a number of tasks on the remote machine, including deleting and moving files, shutting down Windows, logging off users and hiding or killing applications, Windows and processes.

Officials at Wachovia Corp., in Charlotte, N.C., which now owns First Union, said they first became aware of the scam in mid-April and have had some reports from customers who have been affected by it.

"We've had some luck working with the authorities on this, but it's in their hands at this point," said Sandy Vasseur, a spokeswoman for Wachovia. "We don't know if any actual customer PCs were infected. But it's a credibility issue for us. We need to make it clear that this isn't from us."

Vasseur said Wachovia never sends account information in e-mail messages.

-----Original Message-----
From: FDIC [mailto:Waverly_Nikki@gte.net]
Sent: Monday, January 26, 2004 11:10 AM
To: quinn@borg.com
Subject: Important News About Your Bank Account

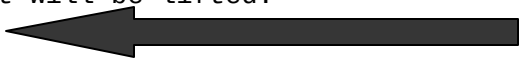
Email used in recent "phish" that sent responders to a fake FDIC website.

To whom it may concern;

In cooperation with the Department Of Homeland Security, Federal, State and Local Governments your account has been denied insurance from the Federal Deposit Insurance Corporation due to suspected violations of the Patriot Act. While we have only a limited amount of evidence gathered on your account at this time it is enough to suspect that currency violations may have occurred in your account and due to this activity we have withdrawn Federal Deposit Insurance on your account until we verify that your account has not been used in a violation of the Patriot Act.

As a result Department Of Homeland Security Director Tom Ridge has advised the Federal Deposit Insurance Corporation to suspend all deposit insurance on your account until such time as we can verify your identity and your account information.

Please verify through our IDVerify below. This information will be = checked against a federal government database for identity verification. This only takes up to a minute and when we have verified your identity you will be notified of said verification and all suspensions of insurance on your account will be lifted.
http://www.fdic.gov=01@211.191.98.216:3180/index.htm
http://www.fdic.gov/idverify/cgi-bin/index.htm



Address appears to be legitimate but after the http://www.fdic.gov the address that follows routes users to a server located at 211.191.98.216

Failure to use IDVerify below will cause all insurance for your account to be terminated and all records of your account history will be sent to the Federal Bureau of Investigation in Washington D.C. for analysis and verification. Failure to provide proper identity may also result in a visit from Local, State or Federal Government or Homeland Security Officials.

Thank you for your time and consideration in this matter.

Donald E. Powell
Chairman Emeritus FDIC
John D. Hawke, Jr.
Comptroller of the Currency
Michael E. Bartell
Chief Information Officer

Threats to Your Business

Internal

- Employee Theft of Cash, Checks, Information
- Manipulation of Ledgers and Bank Statements to conceal activity
- Collusion with Outsiders
- Theft of Incoming and Outgoing Mail
- Establishing Fraudulent Accounts in Company’s Name
- False Invoicing for Services Rendered
- Issuing Unauthorized Checks / Padding Payroll

Threats to Your Business

External

- Theft of Mail to Obtain Bank Information
- Fraudulent Check Orders through Mail Order Houses
- Counterfeit Checks created with PC's and stock purchased at any office supply store
- Dumpster Diving
- Paying for Services or Goods with Fraudulent Checks
- Cleaning Company Employees
- Burglary – Theft of Checks from back of book in Check Stock
- New Electronic (ACH) transactions will make it easier to attack corporate accounts

Business Identity Theft

Business Accounts including commercial accounts are also subject to identity theft from internal and external sources. Accordingly, we strongly recommend a proactive partnership and regular dialogue with your Bank on the vulnerabilities and protection options.

Typical Identity related schemes impacting business and commercial accounts:

- **Misuse or unauthorized transactions on existing business accounts – theft of checks, alteration of checks, unauthorized issuance of checks, unauthorized wire transfers, etc. – Typical Bookkeeper Fraud**
- **Misuse of "proxy identifiers" like account numbers; card numbers; PIN; Passwords; tokens; Company information like TIN; transaction data, etc.**
- **Use of Counterfeit checks and/or ACH transactions – Watch those inclearing items.**
- **Account takeover by impersonation – use of internal position or proprietary knowledge to take over transactional access to the accounts**
- **Opening accounts in the name of your business for the purpose of stealing checks or transferring funds, assets, or usurping your good credit, etc.**
- **Theft and/or misdirection of accounts receivable checks and /or lockbox items by officers and employees of your firm.**
- **Sale of any internal information on your accounts, customers, officers, employees, check copies, signature exemplars or authentication devices, etc. to organized fraud rings.**

Liability Issues

- Lack of control of check stock
- Lack of control of signature facsimile device
- Lack of timely bank statement reconciliation
- Lack of timely notification to bank (30 days)
- Failure to supply current authorized signer documentation to bank and/or notify us when a key executive leaves your company
- Failure to close accounts after loss/theft of checks or unauthorized activity
- Failure to properly destroy check stock or confidential internal documentation
- Lack of internal audit policies
- Lack of prudent hiring practices
- Lack of segregation of duties

Business Partners Should:

Understand the “Rules of Engagement” regarding financial accounts:

- Read & Understand Your Customer Account Holder Agreement & Addendums
- Talk to your banker on fraud issues and discuss the various account protections and products that may be available to reduce risk – i.e. Positive Pay; special account restrictions on debits and credits, etc.
- Understand Uniform Commercial Code Issues which may determine your liability in the event of an identity compromise
- Understand State Laws regarding comparative negligence and how this may influence your responsibilities in the fraud arena – especially on losses or incidents involving your own employees and negligence.
- Understand whether it is appropriate to use business insurance as a risk mitigation option and if so how to best structure your coverage – for both internal involvement and external compromise

Business Partners Should:

Understand your own security posture and take steps to improve controls

- Create a strong control environment – especially related to:
  - Bank and Financial Accounts – Protect your check stocks, signature devices, access devices, PINs, passwords, codes, security tokens, statements, and cancelled checks – Appropriately secure the materials and assign personal accountability, inventory control, and audit control over the materials
  - Implement Strong Segregation of Duties – over access to check stock and bank information; access to signature/authentication/authorization devices; issuance of checks, wire transfers, or other authorizations; daily, weekly, monthly reconcilement responsibilities; etc.
  - Make sure that your authorized signature cards with up-to-date signatories are accurate and on file with your bank Always verify after submission – if you have special circumstances like an officer or business partner "gone bad" – be sure to let your banker know as soon as possible if accounts are potentially at risk.
  - Implement appropriate controls over sensitive data
  - Shred or use a bonded data destruction service for disposal of sensitive proprietary data and financial or bank information.

Minimizing Your Exposure

- Use Positive Pay
- Use check stock with fraud resistant paper safety features and understand limitations
- Review account statements and canceled checks
- Secure check stock & limit access
- Use system passwords and protect them
- Secure access codes for wire transfer, etc...
- Keep your signature cards and related bank information up to date – verify with your bank periodically – and shortly after any changes to signature to insure changes were received and updated on Bank file.

Minimizing Your Exposure

- Review hiring practices (Don’t forget the mailroom staff!)
- Enforce mandatory vacation policies
- Conduct surprise audits
- Segregate duties – especially
  - Check issuance
  - Bookkeeping
  - Financial Statements
  - Receipt of Mail
- Publish and enforce strict integrity policies
- Partner with your bank, accountant, lawyer, and security professional

Wachovia's Fraud Strategy

PREVENTION!!!

- Investment in Technology (43+ fraud prevention strategies)
- Customer Authentication
- "Hot File" systems to interface with teller systems, item processing and other banks
- Account and transaction profiling to detect unusual activity
- Verification Units to assist financial center personnel with suspicious activity

Wachovia's Fraud Strategy

- Centralized Loss Management Department with balanced staff of financial services operations specialists and law enforcement
  personnel
- Partnerships – Loss Management, Operations, Relationship Managers, Wachovia Securities, Wealth Management, etc.
- Strategic Focus with industry peers to pool resources
- Continuous trend analysis balanced with expedient fraud mitigation response

Wachovia's Fraud Strategy

- Field Investigators on the street interfacing with customers and law enforcement
- Commitment to prosecute where warranted
- Ongoing fraud prevention education for front line and back office staff
- Customer Education Seminars
- Wachovia Security & Identity Theft Protection℠
  - "Customer Fraud Assistance Program"
  - Educational Brochures
  - Wachovia.com – Customer Protection & Public Education
  - Security and Identity Theft Newsletter
  - Identity Guard Credit Protect X3 (ID Theft Insurance)
- Identity Theft Assistance Center (ITAC) – Founding Member